

UNITED STATES DISTRICT COURT

MAR 03 2020

for the
Middle District of Tennessee

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*One cellular telephone utilizing cellular telephone number
615-924-7930, which is believed to be possessed by WAYNE
SMITHSON at his residence, 209 Kimela Drive, Woodbury,
Tennessee, in the Middle District of Tennessee.

DEPUTY CLERK

- 1026
Case No. 20-MJ-4024-

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Middle District of Tennessee, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. 2422(b)*Offense Description*
Attempted Enticement of a Minor

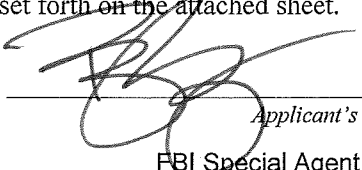
18 U.S.C. 2251

Attempted Production of Child Pornography

The application is based on these facts:

See Attachment C

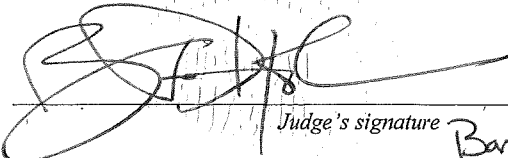
- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

FBI Special Agent Bradley J. Smith

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/03/2020City and state: Nashville, Tennessee
Judge's signature

United States Magistrate Judge Alistair E. Newbern

Printed name and title

Attachment A

Descriptions of Items to Be Searched

One cellular telephone utilizing cellular telephone number 615-924-7930, which is believed to be possessed by WAYNE SMITHSON ("Suspect") at his residence, 209 Kimela Drive, Woodbury, Tennessee, in the Middle District of Tennessee.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

BIS

Attachment B

Items to Be Seized

Materials that constitute evidence of the commission of criminal offenses, or contraband, the fruits of crimes, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, namely violations of 18 U.S.C. §§ 2251, 2252A, 2422(b), and 1470, including but not limited to the following:

1. Any records or other items, including electronic correspondence, pertaining to the transmission, distribution, receipt, solicitation, advertising, or possession of child pornography as defined in 18 U.S.C. § 2256(8); visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); child erotica; a sexual interest in children; enticement of a minor; or sexual activity involving children.
2. Any records or other items pertaining to any minor depicted engaging in sexually explicit conduct.
3. Correspondence, "trophy," grooming aids, and/or other items demonstrating an interest in the exploitation of children.
4. Any visual depictions of minors.
5. Items containing or displaying passwords, access codes, user names, or other identifiers necessary to examine or operate items, software, or information seized.
6. Records of Internet activity, including caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
7. Any electronic records or other items evidencing possession, use, ownership, or access to the SUBJECT DEVICE including, but not limited to, electronic sales receipts, bills for utilities and Internet/online access, credit card receipts, and rental agreements and other identification documents.

Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Attachment C
Statement in Support of Search Warrant

I, Bradley Smith, being first duly sworn, do depose and state as follows:

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2009. During my time as an FBI Special Agent, I have worked a wide variety of federal criminal matters to include white collar crime, public corruption, narcotics offences, violent crimes, and other matters. In the course of these duties, I have been the affiant on numerous federal search warrants. I currently am assigned to the FBI Memphis Division, Clarksville Resident Agency where my primary responsibilities are investigating cases of child exploitation under Title 18, United States Code, Section 2251, et seq.
2. As part of my daily duties, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, and 2252A. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.
3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, and the extraction from that property of electronically stored information described in Attachment B. Specifically, this statement supports an application for a warrant to search an electronic device (the "**SUBJECT DEVICE**") that is a cellular telephone utilizing telephone number 615-924-7930, which is believed to be possessed and utilized by WAYNE SMITHSON ("**Suspect**"), whom resides at an address within the Middle District of Tennessee.
4. The purpose of this application is to seize evidence of violations of 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography; violations of 18 U.S.C. § 2252A(a)(2), which makes it a crime to distribute or receive child pornography in interstate commerce by computer; 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport or ship child pornography in interstate commerce; 18 U.S.C. § 2251, which makes it a crime to manufacture, advertise, or request the production of child pornography, 18 U.S.C. § 2422(b), which makes it a crime to entice a minor to engage in unlawful sexual conduct, and 18 U.S.C. § 1470, which makes it a crime to transfer obscene material to a minor
5. I am familiar with the information contained in this statement based upon the investigation I have conducted, facts related to me by other law enforcement officers, and my conversations with other law enforcement officers who have engaged in numerous investigations involving child exploitation and child pornography.

6. Because this statement is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252A, and 1470 are located in the SUBJECT DEVICE now stored and secured on SUBJECT DEVICE, which is believed to currently be in the possession of Suspect at his residence in the Middle District of Tennessee.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2251, 2252A, 2422(b), and 1470 are present and will be located in the SUBJECT DEVICE on Attachment A.

Child Exploitation Crimes - Statutes and Nature of Offenders

8. In my capacity as an investigator of criminal violations relating to child exploitation and child pornography, I have become familiar with the following federal statutes:
 - a. Transportation of Child Pornography, 18 U.S.C. § 2252A(a)(1), which makes it unlawful for someone to knowingly mail, or transport or ship using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography.
 - b. Receipt and Distribution of Child Pornography, 18 U.S.C. § 2252A(a)(2), which makes it unlawful for someone to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
 - c. Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B), which makes it unlawful for someone to knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means.
 - d. Production of Child Pornography, 18 U.S.C. § 2251(a), which makes it unlawful for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, or transport any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if that person knows or has reason to know that such

visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

- e. Pursuant to 18 U.S.C. § 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”
 - f. Pursuant to 18 U.S.C. § 2256(1), the term “minor,” as “any person under the age of eighteen years.”
 - g. Transfer of Obscene Material to Minors, 18 U.S.C. § 1470, makes it a crime to use the mail or any facility or means of interstate or foreign commerce, knowingly transfers obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so.
9. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography:
- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
 - b. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of electronic photographs and/or videos capturing or describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including cell phones. Many of these individuals also collect child erotica, which consists of

items that may not rise to the level of child pornography but which nonetheless serve a sexual purpose involving children. These individuals often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer to peer ("P2P"), e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces.
- d. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained on electronic devices.
- e. Most individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals may also maintain their collections on password-protected or encrypted electronic devices.
- f. Possessors, traders and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts such as DropBox or iCloud. Therefore, any records, documents, invoices and materials in any format or medium that concern online storage or other remote computer storage could indicate that a person at the Subject Premises is storing illegal material in an online storage account.
- g. Files, logs, and records relating to P2P files can contain the names of files sent through the P2P service, as well as the date and time the files were transferred. These records can help identify the individual who transferred the child pornography images. Additionally, these records can provide historical information about the trading of child pornography by individuals at the Subject Premises.

Relevant Definitions

10. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, communications between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). In addition, the individual can visit websites (see definition of "websites" below), and make purchases from them. Additionally, digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address; and examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.
11. Set forth below are some definitions of technical and other terms, used throughout this statement, and in Attachments A and B hereto, pertaining to the Internet, telephones, and child exploitation cases.
 - a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
 - b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. Sexually Explicit Conduct: Sexually explicit conduct includes actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any persons.
- i. User name or User ID: Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users. User names and ids are typically associated with additional user information or resources, such as a user account protected by a password, personal or financial information about the user, a directory of files, or an email address.
- j. Visual Depictions: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image.
- k. Website: A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Computers and Child Pornography

- 12. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways.

13. Producers of child pornography can now produce both still and moving images directly from a common video, digital camera, and other devices that create video and still images, including most cellular telephones and Personal Digital Assistants ("PDA"). Images and videos from such devices can be transferred easily to a computer using a hard-wired connection or through a wireless connection. Once on the electronic device, images can then be stored, manipulated, transferred, printed, or transferred to other devices or the Internet. Images and videos also can be edited by manipulating the lighting, cropping, or manipulating in some other way. Because of these technologies, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large of an evidence trail for law enforcement to follow.
14. The Internet allows any electronic device to connect to another electronic device. Electronic contact can be made to literally millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child pornography materials with peer-to-peer ("P2P") file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.
15. People who view and collect child pornography often highly prize their collection and will store some or all of their collection on such small, portable computer media, which can be easily hidden and/or transported due to the size of the media. For example, in addition to storing child pornography collections on and near their computers, such people often also store their child pornography computer on smart phones. Such secure storage is readily transportable and makes it unlikely that others will discover their criminal activity.
16. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools.

This is so because when a person “deletes” a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

17. Wholly apart from user-generated files, electronic storage media, including a device such as a smart device, contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
18. Many individuals who collect and traffic child pornography also collect child erotica, which consists of items that may not rise to the level of child pornography but which nonetheless serve a sexual purpose involving children. Such individuals also often collect written stories about sexual activity involving children.

In light of these concerns, I respectfully request the Court’s permission to search the SUBJECT DEVICE described more fully in Attachment A. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

Background on Wildec, LLC

19. Based upon my training and experience, Wildec, LLC is a Miami, Florida-based developer of mobile applications or “apps” for both Apple and Android type smartphones. Many, but not all, of the mobile applications developed by Wildec, LLC are online dating applications. Some of the mobile applications produced by Wildec, LLC, which are pertinent to this search warrant application, include “Meet24,” “FastMeet,” “Meet4U,” and “MeetEZ.” Based upon my training and experience, these four applications appear to act in harmony with each other, with many users utilizing the same or similar online dating profiles on one or more of these applications at the same time. In my experience, while utilizing one of these applications, for example Meet24, a user is able to view the profiles created/maintained on Wildec LLC’s other applications such as FastMeet or Meet4U and have conversations and interactions with these users across the various platforms.
20. Based upon my training and experience, profiles on these relevant Wildec, LLC applications are frequently created, modified, and deleted by users. It is not uncommon

for users to change their profile photos, profile names, ages, and physical locations. While some users may utilize only one single account for a long period of time, other users may utilize numerous accounts. It also is not uncommon for users to create a new account each time they intend to use the application and then delete their profile when they are finished using the application for that session. Because of this, some users can be difficult to track because they are utilizing multiple accounts, change accounts frequently, delete their accounts frequently, and may even change the name or user name(s) on their accounts.

21. In May 2019, it was widely reported that the Federal Trade Commission ("FTC") issued a warning that three of these apps, Meet24, FastMeet, and Meet4U, appeared to violate the Children's Online Privacy Protections Act. Media reports stated that, in a letter sent by the FTC to Wildec, LLC, the FTC said that these apps did not prevent users who say they are under the age of 13 from using the applications or being visible to other users. In response to these concerns, both Apple and Google both temporarily removed these applications for their respective app stores, but the apps were later restored after Wildec, LLC updated their terms and conditions to include that users had to be at least 19 years old to use the applications. However, based upon my training and experience, many users under the age of 19 are still using these applications by misrepresenting their ages to say they are at least 19 years old when in reality they are not.

Investigation

Enticement Conversation Beginning April 8, 2019:

22. On or about April 8, 2019, an FBI certified Online Covert Employee ("OCE") was conducting a covert investigation on the Meet24 online dating application. OCE was utilizing a profile of "Hanna," a 14 year old female from Adams, Tennessee. Hanna's profile contained the photo of a clothed female's face. The female in the photo is an adult Consenting Party who has provided her written consent to allow the FBI use of her photos in online covert child exploitation investigations.
23. On or about April 8, 2019, a Meet24 user utilizing a profile of "Wayne," age 37, from Woodbury, Tennessee ("Suspect") initiated a conversation with Hanna via the Meet24 application by saying, "u need my number." Suspect and Hanna continued to talk via the Meet24 application over the course of a few days. Suspect requested to talk to Hanna via cellular telephone because it was more private and, multiple times, he provided his telephone number of 615-932-0223 to Hanna. Suspect also requested Hanna's age, to which Hanna replied, "I'm 14 like my profile says." After Hanna did not send a text message to Suspect's cellular telephone, Suspect requested, via the Meet24 application, "can i see your pussy ples." Hanna responded that she had "...never taken a pic like that before," to which Suspect responded, "take one ples." Hanna requested "how u want me to take it?" Suspect responded, "with legs open with your titts showing two." Hanna then requested that Suspect send her an example photo of a girl in the pose Suspect was requesting. Suspect then sent Hanna a photo of a nude adult female sitting on a bed with

her breasts and vagina exposed ("PHOTO #1"). The conversation between Suspect and Hanna continued, and Suspect later stated, "just show me pussy" and "just send your pussy only."

24. On or about April 13, 2019, Suspect and Hanna continued their conversation via Suspect's cellular telephone number 615-932-0223. Suspect continued to ask Hanna for nude photos of herself and made requests such as "Can I please see your pussy with your legs open please." After Hanna responded, "I told u I have never taken a pic like that," Suspect replied, "Only one please." The following conversation then took place between Suspect and Hanna on April 13, 2019:

Hanna: Can't u just find pics of 14 year old vagina on the internet?
Suspect: Nope
Hanna: Pretty sure u can
Suspect: No show just show me yours please see if like to eat it

The conversation between Suspect and Hanna later continued on April 13, 2019:

Hanna: How old r u really?
Suspect: 37
Hanna: Wouldn't u rather have some girl ur own age with huge boobs or something?
Suspect: Nope
Hanna: Y not?
Suspect: I like young pussy

Interview of Suspect:

25. On April 23, 2019, I interviewed Suspect at his residence in Woodbury, Tennessee, in the Middle District of Tennessee. Suspect stated that he recalled talking to Hanna. Suspect stated he was not sure of Hanna's age, but believed she was 13 years old. Suspect confessed to asking Hanna to send naked photos of herself, including photos of her vagina. Suspect confirmed that he was the person responsible for the chats with Hanna on both the Meet24 application and via his telephone number. Suspect stated he was the only person who used his telephone number. Suspect stated that he knew it was wrong and illegal to ask 13 or 14 year olds for photos of their vaginas.
26. Suspect provided his written consent to allow me to search his cellular telephone, which was forensically extracted and then placed into evidence. Suspect's phone contains voluminous amounts of text messages, other communications, and images and videos of pornography. Much of this pornography appears to be of adults, but some videos containing what appears to be child pornography have been recovered. On Suspect's phone, I located Hana's telephone number and text message communications between Suspect and Hanna.

Enticement Conversation Beginning June 5, 2019:

27. On or about June 5, 2019, an FBI OCE was conducting a covert investigation on the Meet24 online dating application. OCE was utilizing a profile of "Becca," a 19-year-old female from Clarksville, Tennessee. As stated earlier in the affidavit, as of approximately May 2019, Meet24 altered its terms and conditions that users now had to state they were at least 19 years old to use the application. Becca's profile did not contain any profile photos.
28. On or about June 5, 2019, a Meet24 user with a profile of "wayne," age 37, from Woodbury, Tennessee ("Suspect") initiated a conversation with Becca via the Meet24 application. The conversation on Meet24 was short, with Suspect requesting to talk to Becca via her cellular telephone number, which Becca provided. Suspect and Becca then continued their conversation via text messaging via Suspect's telephone number 615-924-7930 ("**SUBJECT DEVICE**") as follows:

Becca: How old r u?
Suspect: I'm 37
Becca: Cool. Send me a pic
Suspect: Naked picture
Becca: Lol if u want. I'm 15 if u care...
Suspect: Can I see you naked

29. Suspect and Becca continued their conversation on June 5, 2019 via SUBJECT DEVICE. Becca asked for another picture of Suspect, to which Suspect replied, "Show me u naked first." Becca responded, "Honestly I've never taken naked pics before." Suspect sent a message soon after requesting, "Can I see your titts." Becca again reminded Suspect that she was 15 years old and Suspect requested to have "video phone sex" with Becca. Suspect and Becca then agreed to continue their conversation via the mobile application Snapchat.
30. On June 5, 2019, Suspect and Becca continued their conversation via Suspect's Snapchat account, vanity name "Waynesmithson," user name "waynesmithson33." Suspect began the Snapchat conversation by saying, "This is Wayne from Meet24," "Can we do video phone sex now." During this Snapchat conversation, Suspect sent a photo of his partial face and a photo of an adult male's erect penis, which was followed by the following conversation via Snapchat:

Becca: What u gonna do with that lol
Suspect: Let's do video phone sex
Becca: Ok what u want me to do?
Suspect: Call me

Suspect then attempted to initiate video call with Becca, via Snapchat. Becca did not answer the call. Suspect again attempted to initiate a video call with Becca. Becca

briefly answered the call before ending it. Suspect's face was visible during the short duration of this call. After Becca informed Suspect that Becca's mother was home and Becca needed to go, Suspect again asked Becca, "Can I see your pussy." Becca then informed Suspect that she had "never taken pics like that." Suspect told Becca to "Take it with your phone." Becca then requested that Suspect send Becca example photos from the Internet of the pose Suspect wanted Becca to do.

31. Later in the day, on June 5, 2019, Suspect sent Becca six photos of nude adult women, via Snapchat. Five of these photos showed nude females with their face, breasts, and vagina's exposed. The final photo showed only a woman's vagina being held open with her hands and what appeared to be a liquid coming out of the woman's vagina. One of these photos appears to be the same as PHOTO #1 referenced above, which had been sent to Hanna by Suspect in April 2019.

Enticement Conversation Beginning January 20, 2020:

32. On or about January 15, 2020, an FBI OCE was conducting a covert investigation on the Meet24 online dating application. OCE was utilizing a different profile of "Becca," a 47-year-old female from Clarksville, Tennessee. This profile did contain a profile photo of a fully clothed female's face, with her hair partially obscuring her face. The woman in this photo is an adult Consenting Party who has provided her written consent to allow the FBI use of her photos during online covert child exploitation investigations.
33. On or about January 15, 2020, a Meet24 user with a profile of "wayne," age 38, from Woodbury, Tennessee, initiated a conversation with Becca. Suspect and Becca had a brief conversation via Meet24 before moving the conversation to text messaging using the phone number 615-924-7930, the same SUBJECT DEVICE used in June of 2019. The chats contained in this Meet24 conversation between Suspect and Becca were not retained, as Suspect's Meet24 profile was "blocked for violating our service terms & conditions."
34. Becca advised Suspect she could be reached at phone number xxxx. When Suspect texted Becca at phone number xxxx, the phone number associated with the SUBJECT DEVICE (x7930) appeared on the text message. The conversation between Suspect and Becca then continued via SUBJECT DEVICE as follows:

Suspect:	This is Wayne from Meet24
Becca:	Wayne who?
Suspect:	Smithson
Becca:	Oh yeah we just talked sorry.
Suspect:	Ok
Becca:	I Becca. I'm 14 years old. I live in Tennessee.

Suspect went on to state that he was 38 years old and again requested Becca's age, to which Becca replied, "I already said. I'm 14." The conversation continued and Suspect

requested to see Becca in her "...bra underwear on please." The conversation then continued as follows:

Suspect: Can I show you something
Becca: If u want I guess

[Suspect then sent a photo of a purple or pink plastic device on someone's hand]

Becca: Wats that?
Suspect: I put it on my dick if goes into your pussy
Becca: I don't see how that's possible
Suspect: Can I see your pussy

The conversation between Suspect and Becca continued via text messaging on SUBJECT DEVICE. Suspect asked Becca if she liked "video phone sex" and requested to see Becca "fully naked babe" and "One full titts and pussy one with your legs open."

Other Investigation and Identification of Suspect

35. On December 9, 2019, I served an Administrative Subpoena on Snapchat for subscriber information for the Snapchat account vanity name "Waynesmithson," user name "waynesmithson33." On December 19, 2019, Snapchat provided a return that contained limited information but did provide a telephone number associated with the account as 615-932-0223 and an email address of waynesmithson33@gmail.com.
36. On January 27, 2020, I served an Administrative Subpoena on Verizon Wireless regarding subscriber information related to telephone numbers 615-932-0223 and 615-924-7930 (SUBJECT DEVICE). On February 4, 2020, Verizon Wireless provided a return that stated the subscriber for both of these cellular telephone numbers was Wayne Smithson, 209 Kimela Drive, Woodbury, Tennessee. This address is the same location where I interviewed Suspect in April 2019.
37. I also have obtained the Tennessee driver license photo for Wayne Smithson, date of birth 9/xx/1981, listed address of 209 Kimela Drive, Woodbury, Tennessee. Based upon my review of Smithson's Tennessee driver license photo, it closely resembles Suspect's photo contained in all three of his Meet24 profiles, to other photos sent by Suspect to Hanna and Becca, and to images of Suspect captured via Snapchat video calls. All of these photos closely resemble the Wayne Smithson I interviewed at his residence in April 2019.

Indictment

38. On February 26, 2020, Suspect Wayne Smithson was indicted by a federal grand jury in Nashville, Tennessee on a total of seven counts of Attempted Enticement of a Minor (18

U.S.C. §§ 2422(b)), Attempted Production of Child Pornography (18 U.S.C. §§2251(a) and 2251(e)), Attempted Enticement of a Minor (18 U.S.C. § 2422(b)), and Attempted Transfer of Obscene Material to a Minor (18 U.S.C. § 1470), which is directly related to the investigation discussed in this affidavit. The indictment currently is sealed. As of the date of this application, Suspect has not yet been taken into federal custody.

Conclusion

39. Based on the above information, I respectfully submit there is probable cause to believe that there will be evidence of violations of Title 18 U.S.C. §§ 2251, 2252A, 2422(b), and 1470 on SUBJECT DEVICE, which is believed to be a cellular telephone utilizing telephone number 615-924-7930 and in the possession of Suspect WAYNE SMITHSON at his residence in the Middle District of Tennessee, as further described in Attachment A.